OUTLINE

TELECOMMUNICATIONS REQUIREMENTS

Requirements for Common User Networks

effectively Intell- only network

misroute protection mechanisms

spoofing protection mechanisms

minimum of backbone encryption, end-to-end "nice"

Accreditation Issues

Either:

The parties who are exchanging traffic across the network jointly accredit the system, or;

The decision of a community DAA (e.g., large common-user programs, such as AUTODIN, will commonly form multi-agency/department, and multi-community security review and accreditation groups) can be accepted.

Requirements for Internetting

positive identification of other host, and determination/authentication of its clearance level, compartmentation authorizations, and authorized capabilities. Capabilities (e.g., programming) should be controlled accordingly.

the principle of individual accountability should be followed to the maximum extent feasible, although it is realized that it may sometimes be necessary to grant access on the basis of a group identifier.
Individ acct. is the goal to be striven for.

COMMUNICATIONS REQUIREMENTS

a. Network Requirements

This section deals with the issue of connecting an Intelligence community host to any communications system which is not a dedicated community resource. Thus, it applies to those cases in which Foreign Intelligence must be communicated across a common-user backbone communications system, or communications resources in which the intelligence community members appear as "tenants" or customers, and defines the capabilities which a network must provide in order to allow Intelligence community data to be passed across it.

- When the communications are wholly owned, operated, and managed by the Intelligence community it may be assumed that the minimum requirements of this section have been satisfied, and no further analysis of communications security features and capabilities will be required.

- The network must present to the Intelligence community an effectively dedicated network. That is, it must incorporate mechanisms for assuring that intelligence traffic which is injected into the network cannot appear at a non-intelligence community terminal device (i.e., host or terminal) and, moreover, that only a valid intelligence community terminal device can insert traffic labelled as foreign intelligence, to be delivered to an community terminal device. Examples of such mechanisms are the R/Y separation of AUTODIN, and end-to-end encryption. (Note: this is not meant to disallow the identification of a terminal device as being able to appear in several communities, such as Intelligence and GENSER, as necessary. However, the network should be able to control its communications accordingly.)

- The network must provide mechanisms directed toward the prevention of misroutes; it must provide reasonble guarantees that traffic will be delivered to the intended recipient and, more importantly, that it is not delivered to a destination which is not properly cleared for the level and category of traffic. The AUTODIN class-marking mechanism is an example, and end-to-end encryption, with an appropriate key distribution scheme would have the same effect. With modern communications technology it is not unreasonable to expect misroute probabilities not to exceed 1 in 10**10.

- The network must provide anti-spoof protection; it must incorporate mechanisms which prevent/detect a terminal device from masquerading as a different network terminal device, or as a member of a community to which it does not legally belong. The network should be able to provide the receiver positive identification of the identity of the sender.

b. Host Requirements

This next section deals with the requirements which must be satisfied by the Intelligence community host which must operate as part of a network, and which provides capabilities and data to other (non-local) users in the network.

- The host must make positive identification of the distant host with which it is communicating, its identity, its clearance level and compartment approvals, its operating mode, and its authorized capabilities. Capabilities (e.g., programming, data retrieval) must be controlled accordingly.

- The principle of individual accountability should be followed to the maximum extent possible. That is, that each network user who is authorized to connect to, and interact with, a host should be individually identified and authorized. Although it is recognized that it may sometimes be necessary to grant access on the basis of group/project identifiers, individual accountability is the goal to be striven for.